Table of Contents

Chapter 1 – Wide Area Workflow GAM

Overview

Introduction   Welcome to *WAWF Group Administrator (GAM)*. Government organizations shall appoint a Group Administrator (GAM) to manage and activate various users in their organization to have access to WAWF data.

Vendors may also appoint a GAM within their company but this is a option for them whereas not for the government.

The GAM may be an individual tasked with security responsibilities or it may be someone else. It is up to the Service/Agency to determine who has this responsibility.

In this guide   In this guide you will learn about how to use Wide Area Work Flow (WAWF) as a Group Administrator (GAM).

This guide covers the following chapters:

Chapter	Title
1	Wide Area Work Flow Overview
2	Administrative Tasks
3	Group Administrator Tasks

Contents   This chapter contains the following topics.

Topic
Additional Information
Benefits
Reference
WAWF Roles

Overview, Continued

Additional Information

This guide will provide you basic information on how to get started in WAWF. For additional information and training on WAWF please go to the following Web pages:

WAWF Production home page – this is the link to the live WAWF database where all functions are performed in a production setting
https://wawf.eb.mil

WAWF Training Database – this is the link to the WAWF training database where all functions are performed in a practice setting that very closely mirrors the WAWF production database
https://wawftraining.eb.mil

WAWF On-line Training Course - this link leads to the WAWF Training web site where users may access the on-line WAWF computer-based training modules
www.wawftraining.com

Benefits

WAWF supports the Department of Defense (DoD) initiatives for paperless payment processing through the use of Electronic Commerce. WAWF meets these initiatives by providing vendors the means to create and submit invoices and receiving report data electronically and government the ability to perform inspection acceptance on-line, then pass the data electronically to the DoD entitlement system for payment.

WAWF provides global accessibility to all WAWF users and eliminates the potential for lost or misplaced documents during the DoD payment cycle.

References

- Department of Defense Reform Initiative Directive (DRID) #43 – Defense-wide Electronic Commerce dated May 20, 1998

- Office of the Under Secretary of Defense memorandum: Subject: Deployment of Wide Area Workflow – Receipt and Acceptance (WAWF), dated April 1, 2002

- Office of the Secretary of Defense memorandum: Subject: Wide Area Workflow Implementation dated February 6, 2003

DFARS 252.232-7003 Electronic Submission of Payment Requests

Overview, Continued

WAWF Roles   The following are the different roles that may be used during the WAWF process.

Vendor. A person, who is authorized under a government contract to create, submit, correct, and view invoices and receiving report documents in WAWF. Vendors access to WAWF is limited by registration under the firm's CAGE Code

Receiver/Inspector. A government representative who is responsible for the receipt of supplies, equipment, and services. A receiver can inspect, receive, reject, correct and view receipt and acceptance transactions in WAWF

Acceptor. A government representative who is responsible for the acceptance of goods or services. The acceptor is authorized to inspect, accept, reject, correct and view receipt and acceptance transactions in WAWF

Local Processing Official (LPO). A government representative who is responsible for certifying documents prior to being forwarded to DFAS. The LPO is authorized to review, certify, and enter lines of accounting data, as required. The LPO role is mandatory for all Department of the Navy entitlement system payments. The role is also used in the miscellaneous payment process for non-contractually-based transactions. This role is optional for others

Government Payment Official. A government representative who is responsible for the payment review and processing of documents in WAWF. The payment official can recall, reject, or view documents in WAWF

Group Administration Manager (GAM). The GAM is responsible for activation, deactivation and account maintenance for users who have self-registered under the GAM's assigned structure in WAWF. There are vendor GAMs and government GAMs.

Chapter 2 –Administrative Tasks

Introduction In this chapter you will learn the administrative task performed in WAWF

Contents This chapter contains the following topics.

Topic
GAM Overview for Government
Steps before Self-Registering as a Government GAM
Self-Registering using Public Key Infrastructure (PKI) or Common Access Card (CAC)
Self-Registering using User ID and Password
Logging on to WAWF using Public Key Infrastructure (PKI) or Common Access Card (CAC)
Logging on to WAWF using User Id and Password
Resetting Password
Navigating the Side – Bar Menu ◊ My Profile Maintenance ◊ My Role Maintenance ◊ Adding an Additional Role ◊ Password Maintenance

GAM Overview for Government

Group Structure	The users of WAWF are broken down into groups on five levels. One or more GAM administers each group.

A sample Group Structure is pictured below:
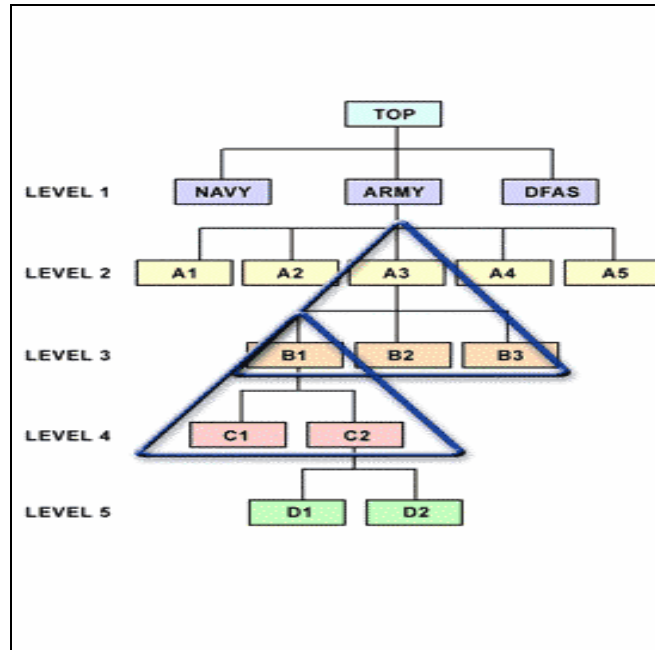
GAM Roles Defined	There are two types of GAMs within WAWF.

- **Group Administrator Manager** - A Group Administrator Manager is at Level 1 of the group structure. This level, called the "Organizational Level," represents the various Service/Agency Headquarters (e.g. Navy, Army, Marines, Air Force, DCMA, DLA, DFAS, etc.)

- **Group Administrator** – A Group Administrator is at Levels 2, 3, 4 or 5 in WAWF. Group Administrators at Levels 2, 3, 4, or 5 have their authority validated by the GAM one level up before they can be activated to use WAWF

Continued on next page

GAM Overview for Government, Continued

Tiered Jurisdiction The GAM can access user records on two levels: the GAM's own group and all groups one level below.   The triangles on the diagram on the previous page indicate sample spans of control. To access more than two levels, a GAM must register as a GAM for each level.

Multiple Roles A GAM is appointed according to their Agency's business rules governing GAM access and GAM responsibilities. In addition to the GAM role, a GAM may also have the role of inspector, acceptor, certifier, vendor, or pay official depending upon their Agency's business rules governing GAM practices.

Software and Hardware Setup There are additional software or hardware setup requirements to use WAWF. In the rare circumstance that you cannot access our home page Vendor and Government users may refer to information on setup requirements and steps at the WAWF production sites. This information may be accessed at https://wawf.eb.mil. Click **Setting up your Machine**.

Steps before Self-Registering as a Government GAM

Process Overview

If you are a Government GAM (levels 2, 3, 4, 5), the GAM one level above you uses your DD Form 2875 and your GAM Appointment letter to authenticate your position before activating your account as prescribed by your Agency's business rules.

If the Group Structure is Already Established:

- Submit a DD Form 2875 to your designated GAM (see sample in Appendix A)
- The GAM will sign a GAM Appointment Letter and distribute copies to all requiring activities according to your Agency's business rules (see sample in Appendix B)
- You can register in WAWF for a GAM role anytime, but your GAM account will not be activated until all forms are completed according to your Agency's business rules

If Adding a New Group:

After initial set-up, additional Groups (DoDAACs) can be added to your account at any time.

- Submit required documentation to your GAM per your Activity's business rules
- The GAM will approve all required documentation and distribute copies to all requiring activities according to the Agency's business rules
- You can register in WAWF for additional Groups/DoDAACs anytime, but your GAM account will not be updated until all required documentation has been completed according to your Agency's business rules

You will need to work closely with your assigned GAM or your service/agency WAWF POC to complete these requirements.

Self-Registering in WAWF using PKI or CAC

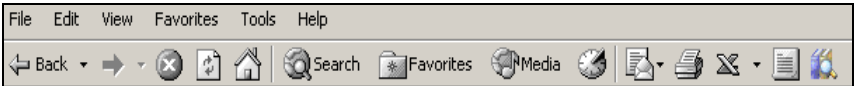**Introduction**   In order to form the GAM functions you will need to self-register as a GAM

Procedure   Follow the steps below to self-register in WAWF using your Common Access Card (CAC).

Step	Action
1	Go to **https://wawf.eb.mil**.
2	Click **Self Register** **Wide Area WorkFlow Training** Version 3.0.7 -- 26 Apr 2005 System Messages: • **Attention: Please disregard the Hardware Signing Module (HSM) Warning. This has already been reported to the WAWF Customer Support.** • This is the WAWF-RA Training System. The WAWF-RA Production System can be accessed at **https://wawf.eb.mil** **Logon** to WAWF (Registered user only) **Self Register** to use WAWF (New users)* **Help** with registration for access to WAWF *Note: Your computer must be set up to run WAWF before you can self register. See "About WAWF." *Result: A message "You are accessing a U.S Government (USG) information system (IS) that is provided for USG authorized use only*."
3	Click **OK** *Result: Warning is displayed alerting you not use the browser back button within the WAWF application*.

Continued on next page

Self-Registering in WAWF using Common Access Card, Continued

Procedure
(continued)

Step	Action
4	Click **OK** WARNING! Please DO NOT use the browser BACK BUTTON within the WAWF application. The use of the browser's BACK BUTTON is not supported within the WAWF application when completing electronic forms. Use of this button will cause the loss of data not yet saved to the server and will result in the application not performing as intended. DO NOT use the backspace key in any uneditable field, as this will function as the back button. Where they exist, use the RETURN or CANCEL buttons to return to a previous page within the WAWF application. OK *Tip: When navigating within the WAWF application, always use the WAWF navigation buttons or hyperlinks to move to new pages or go back to previous pages. Do not use the "Back" and "Forward" buttons provided by your browser, use of these buttons may result in a user being logged out and possible loss of data.* File Edit View Favorites Tools Help Back Search Favorites Media
5	From the WAWF Self Registration form fill in all required data (all fields with the *) **WAWF Self-Registration** * indicates mandatory field First Name* : John Last Name* : Doe Commercial Telephone* : 000 000 0000 DSN Telephone : Rank/Grade (Mandatory for Government Users) : GS E-mail Address* : john.doe@dfas.mil Organization* : Electroinc Commerce Title* : System Specialist Continue Return Page Help
6	Click **Continue**.

Procedure
(continued)

Step	Action
7	Select the radio button labeled **DoD Common Access Card**. **WAWF Self-Registration** * indicates mandatory field Logon Method* ○ User ID and Password ○ DoD or ECA Software Certificate ⦿ DoD Common Access Card Continue Return Page Help
8	Click **Continue**.
9	Click **Select Certificate**. **WAWF Self-Registration** * indicates mandatory field Certificate* Select Certificate Continue Return Page Help *Result: Security Alert screen is displayed.*

Self-Registering in WAWF using Common Access Card, Continued
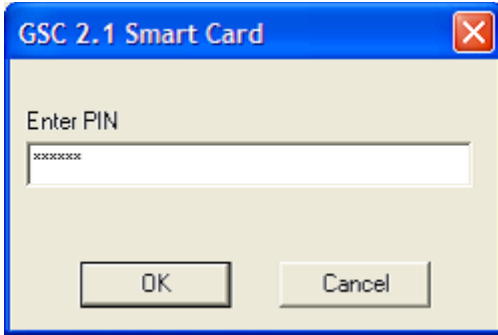
Procedure
(continued)

Step	Action
10	Click **Yes**. **Security Alert** This Web site needs access to digital certificates on this computer. WARNING: By allowing access to your certificates, this Web site will also gain access to any personal information that are stored in your certificates. Do you want this Web site to gain access to the certificates on this computer now? Yes No *Result: Select certificate screen is displayed.*
11	Select the certificate with the user's name and **<ALL>**. **Select Certificate** Select the certificate you want to use. | Issued to	Issued by	Intende...	Friendly...	Expirati...	Location
PLAT...	DOD CL...	<All>	None	9/19/2007	Not avail...
PLAT...	DOD CL...	Smart C...	None	9/19/2007	Not avail...	 OK Cancel View Certificate
12	Click **OK**. *Result: Security alert screen is displayed*.
13	Click **Yes**. *Result: The CAC Smart Card screen is displayed*.

Procedure
(continued)

Step	Action
14	Enter Pin number.
15	Click **OK**.
	Result: WAWF Self-Registration screen is displayed with user name and certificate
16	Click **Continue**.

Procedure
(continued)

Step	Action
17	In the "Role" drop down menu, select **Group Administrator** **WAWF Self-Registration** * indicates mandatory field **Role** Group Administrator Continue Return Page Help *Tip: In the role field, the drop down menu arrow reveals the various roles in the WAWF system. From this list you can select the additional role for which you want to register.*
18	Click **Continue**.

Continued on next page

Self-Registering in WAWF using Common Access Card, Continued

Procedure
(continued)

Step	Action
19	Decide which action you want to take to locate the group you will become the GAM for.

IF	THEN
Enter Group Name	Click Continue

WAWF Self-Registration

* indicates mandatory field

Enter the group name, or use the Lookup Group link to find the group name based on a location code.

Group Name*

DFAS   **Lookup Group**

Continue   Return   Page Help

OR

IF	THEN
Click Lookup Group	Click Continue Enter Location Code Click Lookup Group

WAWF Self-Registration

* indicates mandatory field

Locate the group name by entering a location code that is in the group.

Location Code*

HQ0101

Lookup Group   Return   Page Help

Microsoft Internet Explorer

The location code entered, HQ0101, is in the DFAS group.
Do you wish to register as group administrator of this group?

OK   Cancel

Self-Registering in WAWF using Common Access Card, Continued

Procedure
(continued)

Step	Action
20	Click **Browse** to add an attachment (2875) or you may enter comments in the comments block *Tip: If no comments are attachments are needed go to step 24*
21	Chose file name and click **Open**. *Result: File name will display in the box next to browse*

Continued on next page

Self-Registering in WAWF using Common Access Card, Continued

Procedure
(continued)

Step	Action
22	Click **OK** on the SAM HAM message.
23	Click **Add Attachment.** *Result: Screen will display giving you the capability to View, Delete or add another attachment.*
24	Click **Continue.** *Result: Profile Information screen is displayed*

Continued on next page

Self-Registering in WAWF using Common Access Card, Continued

Procedure (continued)

Step	Action
25	Review the profile information you have entered.
26	*OPTIONAL - If you wish to add additional roles then click on the add icon* *under the Action Column for Role Information. You can edit your profile information by click the edit icon under the Action Column for Profile Information. To delete a role you may have registered for in error click on the delete icon*
27	Click on the check box for **Statement of Accountability** after you have reviewed the Profile and Role Information ensuring everything on the screen is correct.
28	Click the **Register Now** button (you must submit the form for it to be valid). Result: After registration is completed Ogden will automatically email an activation notice to the registrant stating you have successfully been activated. *Important: Upon your GAM activating your account an email will be sent to you. The email will contain a one-time temporary password for your initial logon. You will need to change your temporary password.*

Self-Registering in WAWF using User ID & Password

Introduction   In order to form the GAM functions you will need to self-register as a GAM

Procedure   Follow the steps below to self-register in WAWF.

Step	Action
1	Go to **https://wawf.eb.mil** *Result: Home page screen opens.*
2	Click **Self-Register**. *Result: A message "You are accessing a U.S Government (USG) information system (IS) that is provided for USG authorized use only."*
3	Click **OK** *Result: Warning is displayed alerting you not use the browser back button within the WAWF application.*

Self-Registering in WAWF using User ID & Password, Continued

Procedure (continued)

Step	Action
4	Click **OK**
	WARNING! Please DO NOT use the browser BACK BUTTON within the WAWF application. The use of the browser's BACK BUTTON is not supported within the WAWF application when completing electronic forms. Use of this button will cause the loss of data not yet saved to the server and will result in the application not performing as intended. DO NOT use the backspace key in any uneditable field, as this will function as the back button. Where they exist, use the RETURN or CANCEL buttons to return to a previous page within the WAWF application. [OK]
	Tip: When navigating within the WAWF application, always use the WAWF navigation buttons or hyperlinks to move to new pages or go back to previous pages. Do not use the "Back" and "Forward" buttons provided by your browser, use of these buttons may result in a user being logged out and possible loss of data.
	File Edit View Favorites Tools Help / Back Search Favorites Media
5	From the WAWF Self Registration form fill in all required data (all fields with the *)
	WAWF Self-Registration — * indicates mandatory field First Name*: John Last Name*: Doe Commercial Telephone*: 000 000 0000 DSN Telephone: Rank/Grade (Mandatory for Government Users): GS E-mail Address*: john.doe@dfas.mil Organization*: Electroinc Commerce Title*: System Specialist [Continue] [Return] [Page Help]
6	Click **Continue.**

Procedures
(continued)

Step	Action
7	Click the radio button labeled **User ID and Password.** **WAWF Self Registration** * indicates mandatory field Logon Method * ⦿ User ID and Password ○ DoD or ECA Software Certificate ○ DoD Common Access Card [Continue] [Return] [Page Help]
8	Click **Continue.**
9	Enter in a **"User ID"**. Please create your own. (It must be a minimum of 8 characters long). **WAWF Self-Registration** * indicates mandatory field User ID* wawfuser1 [Continue] [Return] [Page Help]
10	Click **Continue**.
11	In the "Role" drop down menu, select **Group Administrator** **WAWF Self-Registration** * indicates mandatory field Role Group Administrator ▾ [Continue] [Return] [Page Help] *Tip: In the role field, the drop down menu arrow reveals the various roles in the WAWF system. From this list you can select the additional role for which you want to register.*
12	Click **Continue**.
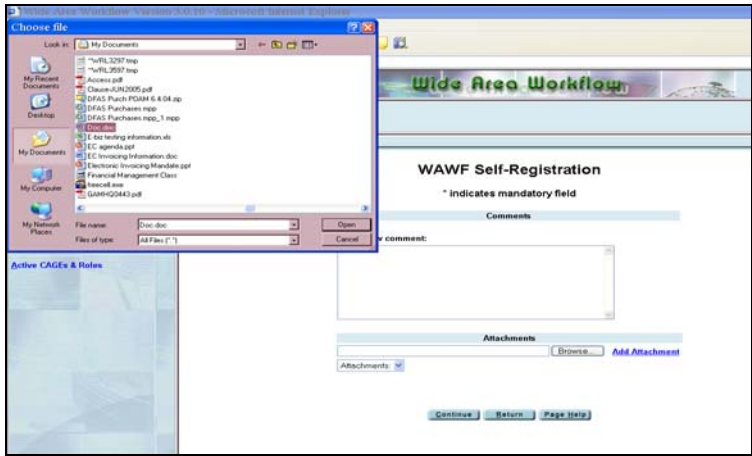
Procedure
(continued)

Step	Action
13	Decide which action you want to take to locate the group you will become the GAM for.

IF	THEN
Enter Group Name	Click Continue

WAWF Self-Registration

* indicates mandatory field

Enter the group name, or use the Lookup Group link to find the group name based on a location code.

Group Name*

DFAS   **Lookup Group**

Continue   Return   Page Help

OR

IF	THEN
Click Lookup Group	Click Continue Enter Location Code Click Lookup Group

WAWF Self-Registration

* indicates mandatory field

Locate the group name by entering a location code that is in the group.

Location Code*

HQ0101

Lookup Group   Return   Page Help

Microsoft Internet Explorer

? The location code entered, HQ0101, is in the DFAS group. Do you wish to register as group administrator of this group?

OK   Cancel

Self-Registering in WAWF using User ID and Password, Continued

Procedure
(continued)

Step	Action
14	Click **Browse** to add an attachment (2875) or you may enter comments in the comments block ![WAWF Self-Registration form with Comments box and Attachments section] *Tip: If no comments are attachments are needed go to step 24*
15	Chose file name and click **Open**. ![Choose file dialog box over the Wide Area Workflow WAWF Self-Registration page] *Result: File name will display in the box next to browse*

Self-Registering in WAWF using User ID and Password, Continued

Procedure
(continued)

Step	Action
16	Click **OK** on the SAM HAM message.
17	Click **Add Attachment.** *Result: Screen will display giving you the capability to View, Delete or add another attachment.*
18	Click **Continue.** Result: **Profile Information** screen is displayed
19	Review the profile information you have entered.

Self-Registering in WAWF using User ID and Password, Continued

Procedure
(continue)

Step	Action
20	*OPTIONAL - If you wish to add additional roles then click on the add icon under the Action Column for Role Information. You can edit your profile information by click the edit icon under the Action Column for Profile Information. To delete a role you may have registered for in error click on the delete icon*
21	Click on the check box for **Statement of Accountability** after you have reviewed the Profile and Role Information ensuring everything on the screen is correct.
22	Click the **Register Now** button (you must submit the form for it to be valid). Result: After registration is completed Ogden will automatically email an activation notice to the registrant stating you have successfully been activated. ***Important**: Upon your GAM activating your account an email will be sent to you. The email will contain a one-time temporary password for your initial logon. You will need to change your temporary password. (See page 43 for password criteria).*

Logging on to WAWF using PKI or CAC

Introduction   In order to do the GAM functionally in WAWF you must Logon. You will need to have self-registered to Logon to WAWF. If you have not already self-registered, refer to procedures on how to self-register in WAWF

Procedure   Follow the procedure below using CAC to access WAWF

Step	Action
1	Go to **https://wawf.eb.mil** Result: WAWF-RA Home page screen is displayed.
2	Click **Logon**. **Logon** to WAWF (Registered user only) **Self Register** to use WAWF (New users)* **Help** with registration for access to WAWF *Result: Warning is displayed alerting you to NOT use the browser BACK BUTTON within the WAWF application.*
3	Click **OK**. WARNING! Please DO NOT use the browser BACK BUTTON within the WAWF application. The use of the browser's BACK BUTTON is not supported within the WAWF application when completing electronic forms. Use of this button will cause the loss of data not yet saved to the server and will result in the application not performing as intended. DO NOT use the backspace key in any uneditable field, as this will function as the back button. Where they exist, use the RETURN or CANCEL buttons to return to a previous page within the WAWF application. [OK] *Tip: When navigating within the WAWF-RA application, always use the WAWF-RA navigation buttons or hyperlinks to move to new pages or go back to previous pages. Do not use the "Back" and "Forward" buttons provided by your browser, use of these buttons may result in a user being logged out and possible loss of data.* File Edit View Favorites Tools Help Back Search Favorites Media

Logging on to WAWF using PKI or CAC), Continued

Procedure
(continued)

Step	Action
4	Click **Select Certificate**. **WAWF - Logon** User Id Password Select Certificate Submit Return Page Help If you have forgotten your WAWF password, please contact your group administrator or Customer Support. *Result: Security Alert screen is displayed.*
5	Select the certificate with the user's name and **<ALL>**. Select Certificate Select the certificate you want to use. Issued to | Issued by | Intende... | Friendly... | Expirati... | Location PLAT... | DOD CL... | <All> | None | 9/19/2007 | Not avail... PLAT... | DOD CL... | Smart C... | None | 9/19/2007 | Not avail... OK Cancel View Certificate

Procedure
(continued)

Step	Action
6	Click **OK**. Result: Security Alert box is displayed
7	Click **Yes**. **Security Alert** This Web site needs to create a digital signature using your private key. WARNING: Allowing an untrusted Web site to use your private key is a security risk. The Web site could use your private key to compromise protected data or assume your identity. Do you want this Web site to create the signature now? ☐ Do not show this dialog box again. If you select this check box, any Web pages within this site will be able to create digital signatures without prompting you again. However, you will be prompted again when you visit another Web site. [Yes] [No]
8	Enter Pin number. **GSC 2.1 Smart Card** Enter PIN xxxxxx [OK] [Cancel]
9	Click **OK**
10	Click **Submit**. **WAWF - Logon** **User Id** _____ **Password** _____ bsm.DF.3010020096 [Submit] [Return] [Page Help] John Doe 0000000000 F password, please contact your group ort. *Result: Certificate with your name screen is displayed*

Logging on to WAWF using PKI or CAC, Continued

**Important -
Session
time-out**

WAWF-RA has a security time-out function that limits the WAWF-RA session to approximately 30 minutes of inactivity. If you have not used WAWF-RA within 25 minutes, a pop-up message activates.

The pop-up window gives you a choice of selecting **OK** to continue working, or Cancel to end the session at the regularly scheduled loss of session (in approximately 5 minutes).

If you do not Click OK when the pop-up window activates, your session will be timed out. All data that you have entered but not submitted will be lost. You must log back in to continue working.
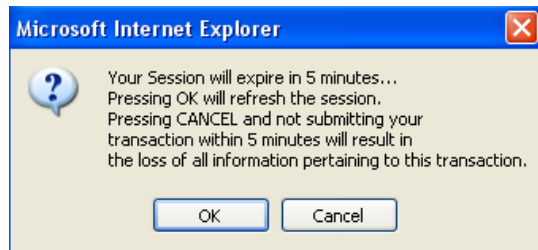
Logging Off

When you are finished working in WAWF-RA, you should log off by returning to the home page and then close your browser.
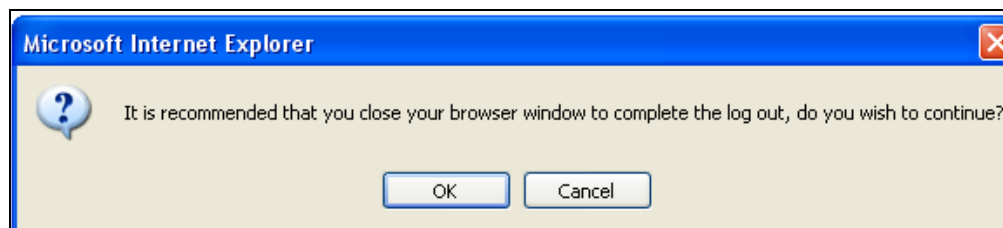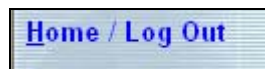
It's important to log off properly for security reasons. If you do not log off, anyone with access to your computer can view and manipulate documents in WAWF.

Logging on to WAWF using User ID & Password

Introduction In order to do the GAM functionally in WAWF you must Logon. You will need to have self-registered to Logon to WAWF. If you have not already self-registered, refer to procedures on how to self-register in WAWF
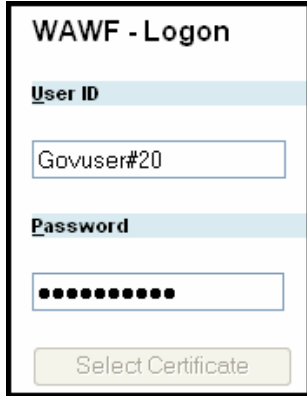
Procedure Follow the steps below to Logon to WAWF using User Id and Password

Step	Action
1	Go to **https://wawf.eb.mil** Result: WAWF-RA Home page screen is displayed.
2	Click **Logon**. **Logon** to WAWF (Registered user only) **Self Register** to use WAWF (New users)* **Help** with registration for access to WAWF *Result: Warning is displayed alerting you to NOT use the browser BACK BUTTON within the WAWF application.*
3	Click **OK**. WARNING! Please DO NOT use the browser BACK BUTTON within the WAWF application. The use of the browser's BACK BUTTON is not supported within the WAWF application when completing electronic forms. Use of this button will cause the loss of data not yet saved to the server and will result in the application not performing as intended. DO NOT use the backspace key in any uneditable field, as this will function as the back button. Where they exist, use the RETURN or CANCEL buttons to return to a previous page within the WAWF application. [OK] *Tip: When navigating within the WAWF-RA application, always use the WAWF-RA navigation buttons or hyperlinks to move to new pages or go back to previous pages. Do not use the "Back" and "Forward" buttons provided by your browser, use of these buttons may result in a user being logged out and possible loss of data.* File Edit View Favorites Tools Help Back · · · · · Search Favorites Media

Continued On Next Page

Logging on to WAWF using User ID & Password ,

Procedure (continued)

Step	Action
4	Enter your **User ID/Password** WAWF - Logon **User ID** Govuser#20 **Password** •••••••••• Select Certificate *Tip: User ID and Password are case sensitive.*
5	Click **Submit** *Results: User menu screen opens*.

Navigating the Side-Bar Menu on the WAWF Home Page – Prior to Log-On

Introduction   The WAWF homepage contains several important links to general information for all users. This information is updated with each new release of WAWF so it will remain current.

Homepage

Homepage   Below is the WAWF homepage. Tip the system messages. These messages will change as needed. It is important to read this each time you log into WAWF so that you stay current on all important information.

Customer Support

Customer Support   The Defense Information Systems Agency (DISA) is available via phone or email for your WAWF technical support. The Help Desk will issue a trouble ticket and work to resolve the problem. Trouble tickets are used to monitor system wide errors and are used to resolve problems and provide immediate assistance for like problems. The left navigation bar on the WAWF Home Page contains contact information for the DISA WAWF Customer Support Help Desk.

About WAWF link

About WAWF link   The About WAWF link contains important links for new users to WAWF

- **Functional Information** – includes background on the system and some of the same information you saw in the overview.

- **Setting Up Your Vista Machine for WAWF with MSIE Brower Version 7 –** includes detail instructions for setting up your computer to use WAWF

- **Using WAWF with MSIE 7 Browser-** includes detailed instructions for setting up your computer to use WAWF.

- **Setting Up Your Machine – Desktop** – includes detailed instructions for setting up your computer to use WAWF.

- **Setting Up Your Machine – Wireless** – includes detailed instructions for setting up your computer to use WAWF on a wireless device.

- **Access Web Based Training** – The Web-based training is an excellent reference and educational site for initial training in WAWF. It also is excellent for refresher training, new releases and when new employees come on board.

- **Frequently Asked Questions** (FAQ)

- **Deployment Checklist** – This deployment checklist is for DoD entities new to WAWF. The checklist identifies 17 steps necessary to begin using the WAWF application.

What's New link

What's New link   Provides information about what is new in WAWF for previous and current system release enhancements.

```
-] What's New
    A. Version 3.0.1
    B. Version 3.0.1.1
    C. Version 3.0.2
    D. Version 3.0.2.1
    E. Version 3.0.2.2
    F. Version 3.0.3
    G. Version 3.0.3.1
    H. Version 3.0.4
    I. Version 3.0.4.1
    J. Version 3.0.5
    K. Version 3.0.6
    L. Version 3.0.7
    M. Version 3.0.8
    N. Version 3.0.9
    O. Version 3.0.10
    P. Version 3.0.11
    R. Version 3.0.12
```
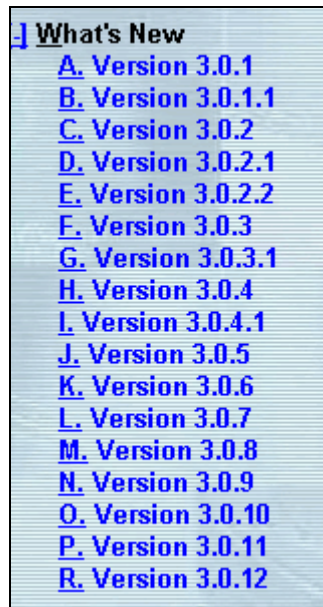
Security & Privacy link

Security & Privacy link   Provides the notice describing the security and privacy of WAWF.

Active DoDAACs & Role link

Active DoDAACs & Role link
The Active DoDAACs & Role link is used when a Government or Vendor user needs to determine if a government activity has active users registered within WAWF.

WAWF Active DoDAACs and Roles

* indicates mandatory field

DoDAAC * [   ]   Extension [   ]

Enter search criteria. Partial entries are NOT acceptable for DoDAAC.

[Submit] [Reset] [Page Help]

Active CAGE Code link

Active CAGE Code link
The Active CAGE Code link is used when a Government user needs to determine if a Vendor has active users registered within WAWF.

WAWF Active CAGE Code

* indicates mandatory field

CAGE Code * [   ]   Extension [   ]

Enter search criteria. Partial entries are NOT acceptable for CAGE Code.

[Submit] [Reset] [Page Help]

My Profile Maintenance

Introduction My Profile Maintenance lets you update the personal profile information on your WAWF account.

Change Profile Information

Procedure Follow the steps below to change your WAWF profile information:

Step	Action
1	**Logon** to WAWF. Result: On left-hand side of the screen the submenu is displayed.
2	Click **My Profile Maintenance**. *Result: Profile information screen is displayed.*

My Profile Maintenance

Change Profile Information

Procedure (continued)

Step	Action
3	Click the **edit icon**, which looks like a pen, under Action in the Profile Information section. **Action** Result: The User Profile Information form is displayed
4	Update personal information. **User Profile** * = Required Fields **First Name*** Gov **Last Name*** Pay **Commercial Telephone*** 1111111111 **DSN Telephone** **Rank/Grade*** gs01 **E-mail Address*** we6dad@cols.disa.mil **Organization*** pay **Title*** pay Continue Return Page Help *Tip: You may change multiple fields of information before you click the Continue button. You can make changes to your personal profile information: your name, phone number, email address, rank, title, or job description.*
5	Click **Continue**. *Result: The Profile Information page appears again*.

My Profile Maintenance

Change Profile Information

Procedures
(continue)

Step	Action
6	Put a check in the checkbox next to **Statement of Accountability**.
7	Click **Submit**. *Result: Message appears stating "Your profile information has been successfully updated."*

My Profile Maintenance

Introduction   Under Logon Information you can change your Logon Type from User ID and Password to Certificate or from Certificate to User Id and Password.

Change Logon Information

Procedure   Follow this procedure to change Logon Information.

Step	Action
1	**Logon** to WAWF. Result: On left-hand side of the screen the submenu is displayed.
2	Click **My Profile Maintenance**. *Result: Profile information screen is displayed.* *Tip: In the bottom section, you can change your method of logging on to WAWF from User ID and password to certificate.*
3	Click the edit icon Action under Logon Type. *Result: Logon Method screen is displayed.*

My Profile Maintenance

Change Logon Information

Procedure
(continue)

Step	Action
4	Select appreciate Logon Method.
5	Click **Continue**.
6	Click **Select Certificate**. *Result: Security Alert box appears.*

Continued on next page

My Profile Maintenance

Change Logon Information

Procedure
(continue)
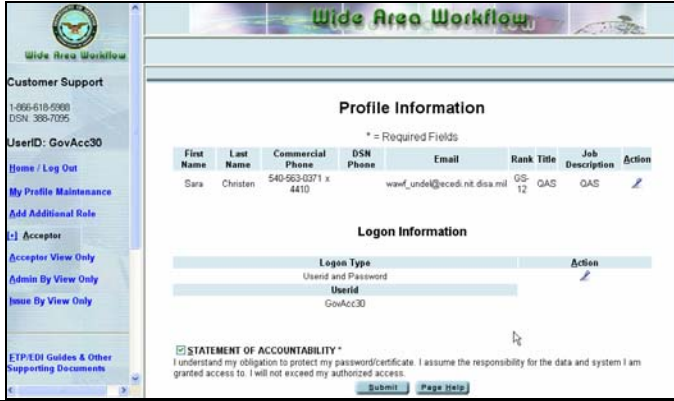
Step	Action
7	Click **Yes**. *Result: Select Certificate box is displayed.*
8	Select the certificate with the user's name and **<ALL>**.

My Profile Maintenance

Change Logon Information

Procedure
(continue)

Step	Action
9	Click **OK**. *Result: Your name is displayed in the Select Certificate box.*
10	Click **Continue**.
11	Put a check in the checkbox next to **Statement of Accountability**.
12	Click **Submit**. *Result: Message appears stating "Your profile information has been successfully updated."*

My Role Maintenance

Introduction   My Role Maintenance gives each user the capability to view all the roles and DoDAAC they are registered for and weather or not you are active.

View Comments

Procedure   Follow the steps below to view roles/comments.

Step	Action
1	**Logon** to WAWF. *Result: On left-hand side of the screen the submenu is displayed.*
2	Click **My Role Maintenance**.
3	Review the information. *Tip: You can sort by Role, Group, Location Code, Extension, Registration Date, Active Status, Comments, and Attachments.*.
4	Click on **View** under Comments/Attachments column.

My Role Maintenance, Continued

View Comments

Procedure
(continued)

Step	Action
5	Review or add comments.
6	Click **Return** Result: Will return back to Role for User

My Role Maintenance, Continued

Introduction At times if attachments are required they are not always added doing initial registration. Under My Role Maintenance there is the capability to view comments and add attachments.

Add Attachment

Procedure Follow the steps to add an attachment.

Step	Action
1	**Logon** to WAWF. ***Result: On left-hand side of the screen the submenu is displayed.***
2	Click **My Role Maintenance**.
3	Review the information. ***Tip: You can sort by Role, Group, Location Code, Extension, Registration Date, Active Status, Comments, and Attachments***
4	Click on **Add** under Comments/Attachments column.
5	Click **Browse** to add an attachment.

Continued on next page

My Role Maintenance, Continued

Add Attachment

Procedure
(continued)

Step	Action
6	Chose file name and click **Open**. *Result: File name will display in the box next to browse*
7	Click **OK** on the SAM HAM message.
8	Click **Add Attachment.** *Result: File name will display in the Attachments drop down box.*
9	Click **Return.** *Result: Will return back to Role for User.*

Adding an Additional Role

Introduction   The link **Add Additional Role** allows you to add additional

- DoDAACs
- MPACs
- User roles

after you have already registered instead of registering again
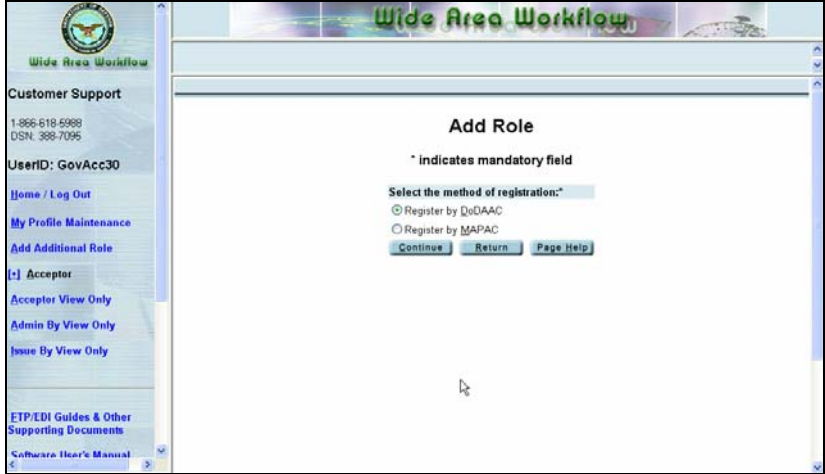
Procedure   Follow the procedure below to add an additional role in WAWF:

Step	Action
1	**Logon** to WAWF *Result: On left-hand side of the screen the submenu is displayed.*
2	Click **Add Additional Role** *Result: The Add Role page opens.*
3	From the drop down list, click on the desired role.
4	Click **Continue**

Procedure (continued)

Step	Action
5	Select the radio button labeled for **DoDAAC or MAPAC** (Military Assistance Program Access) for which you want to register.
6	Enter the **DoDAAC or MAPAC** for which you want to register.
7	Click **Continue**.
8	Click **Browse** to add an attachment (2875) or you may enter comments in the comments block if necessary

Adding an Additional Role, Continued

Procedure
(continue)

Step	Action
9	Click the **Statement of Accountability** checkbox. *Result: The system informs you that your Role Information was **upda**ted*
10	Click **Submit**.
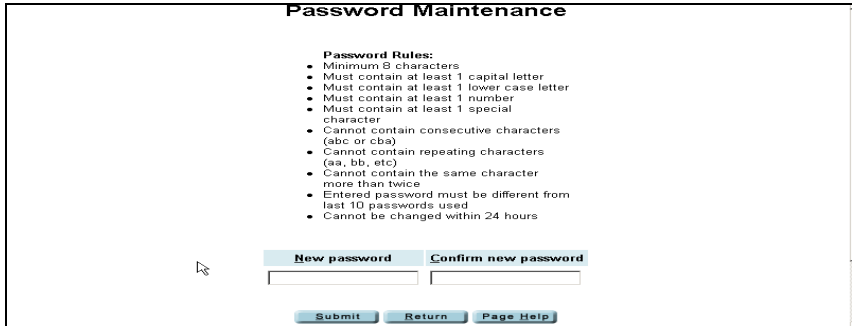
Password Maintenance

Introduction   From the user submenu page, you can change your password at anytime before it expires.

Procedure   Follow the steps below to change your password in WAWF.

Step	Action
1	**Logon** to WAWF. *Result: On left-hand side of the screen the submenu is displayed.*
2	Click **Password Maintenance**.
3	Enter your current password in the text entry box.
4	Click **Continue.** *Result: The Password Maintenance screen is displayed.*
5	Type your new password twice. Password formatting guidelines require that every password must:

Chapter 3 WAWF Group Administrator (GAM) Task

Introduction   The Group Administrator performs an important role in WAWF. The GAM is responsible for activation, deactivation and account maintenance for users who have self-registered under the GAM's assigned structure in WAWF.

Contents   This chapter contains the following topics.

Topic
Group Administrator
Group Structure
Administer Location Codes
Use Group Look-up Function
View User Information
Activate and Deactivate User Account
Activation Report
Reset User Password
Reset User Certificate

Group Administrator

Introduction   After logging into WAWF, the Group Administrator Menu will appear in the middle of the sidebar. This menu provides access to all the functions you can perform as a WAWF GAM.

Tip: When you first log on to WAWF, the Group Administrator menu will be collapsed. To display the submenu, click the plus sign [+] next to the Group Administrator menu title.

Clicking on the plus sign [+] expands the submenu and the sign changes to a minus [-]. The Group Administrator submenus remain visible when you change pages.

To collapse the menu, click on the minus [-] sign.

Group Administrator Submenu   The Group Administrator Submenu consists of the following functions:

| Description of Functions | The table below describes the eight Group Administrator functions. |

Function	Description
Group Structure	Within this section , the GAM has a unique set of actions that permit updating the structure based on current policies and procedures These include: ◊ Administer users in this group ◊ Administer location codes in this group ◊ Moving Location Codes between Groups/Subgroups
Location Codes	Within this section, the GAM can: ◊ View DoDAACs registered under a group ◊ Assign or change an organizational e-mail address fro each DoDAAC or CAGE in the group or extension ◊ Create extension
Group Lookup	Within this section, the GAM can do two things: ◊ View the group name associated with a particular location code (DoDAAC) ◊ View all GAM(s) registered under the location code (DoDAAC)

Group Administrator, Continued

Description of Functions, Continued	

Function	Description
User Information	Within this section, the GAM can: ◊ View user's profile and/or the roles associated with the user, as well as view the date the user registered ◊ Edit the profile to update any portion of the information associated with the users ◊ Add attachment to a user's profile ◊ Achieve any inactive accounts
Activation	Within this section, the GAM can: ◊ Active, deactivate and re-activate users within the GAM's span of control ◊ Review all users accounts under a particular Group Name, Location Code Extension, User role, or User Status ◊ Perform group Activations by pulling all inactive user roles, under a location code
Activation Report	Within this section, the GAM can: ◊ Provide a means for locating the activation history of a specific user via search.
Reset Password	Within this section, the GAM can : ◊ Reset a user's password or guide
Reset Certificate	Within this section, the GAM can: ◊ Reset user's certificate

Group Structure

Introduction   In this section you will learn how to perform the following tasks:

- ◊   Administer users in this group
- ◊   Administer achieved user in this group
- ◊   Administer location codes in this group
- ◊   Move a location code to this group
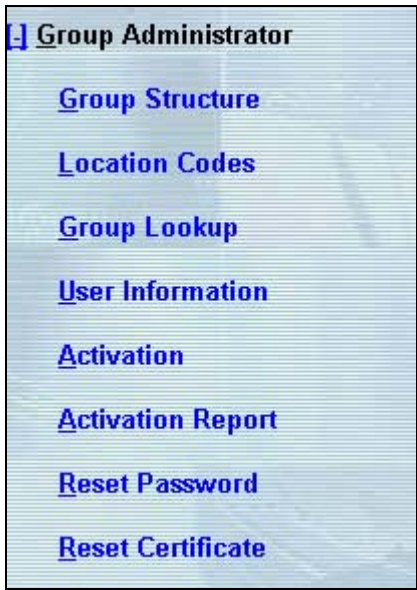
Administer users in this group

Introduction   Use the information from this link to view active users' information from their profile to their roles in that group.

Procedure   Follow the steps below to view active users' information for the users in a group.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **Group Structure.** [-] Group Administrator Group Structure Location Codes Group Lookup User Information Activation Activation Report Reset Password Reset Certificate *Result: Current Group screen is displayed.*

Administer users in this group, Continued

Procedure (continued)

Step	Action
4	Click **Administer users in this group**. **Current Group: VENDOR** **Path to Current Group** TOP / VENDOR **Actions for Current Group** Administer users in this group Administer archived users in this group Administer location codes in this group Move a location code to this group **Subgroups** 02978 32562 3GBT6 *Result: This screen displays all achieve users available under this group. You can view the users Profile and/or Roles*
5	On this screen you can the results are displayed ten a time, labels at the top of the screen indicate the current group and the total number of users, the current page number and page count are at the bottom of the page, a dropdown box and paging button allow you to select the next page to be viewed and you can sort the list of users by User ID by First Name, or by Last Name and in either ascending or descending alphabetical order. **Current Group: VENDOR** **There are 713 users in this group.** **These are users with current roles.** Sort by: Userid ascending Sort |	Userid	First Name	Last Name	Actions	
1	lancourc			Profile	Roles
2	DCMAVEND3	Tester	3	Profile	Roles
3	DPRPV003	Tester	3	Profile	Roles
4	jackson2	333	333	Profile	Roles
5	MHnY55FD	Bianca	A'rmenta	Profile	Roles
6	4N727	Sheila	Adame	Profile	Roles
7	e0874880	LETICIA	AGUILAR	Profile	Roles
8	SIKORSKY	Sikorsky	Aircraft	Profile	Roles
9	benaitken	Benjamin	Aitken	Profile	Roles
10	nilasoni	Leona	Alatini	Profile	Roles	 Page 1 of 72 Go to: Page 2 >> Return to Group Structure *Tip: To view user profile follow steps 6-8.* * To view user Role follow steps 9-11.*
6	Click **Profile** under "Actions" to view user's profile information. *Result: User Information screen is displayed with the user's registration information.*

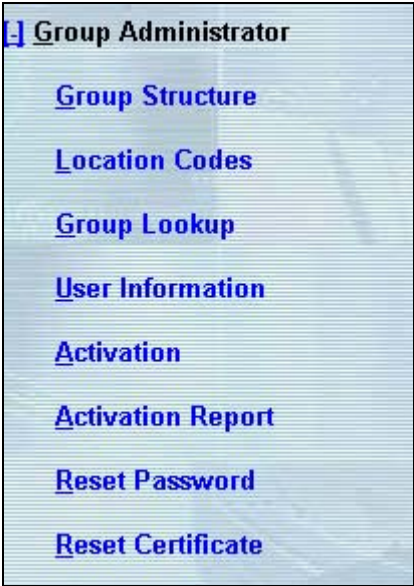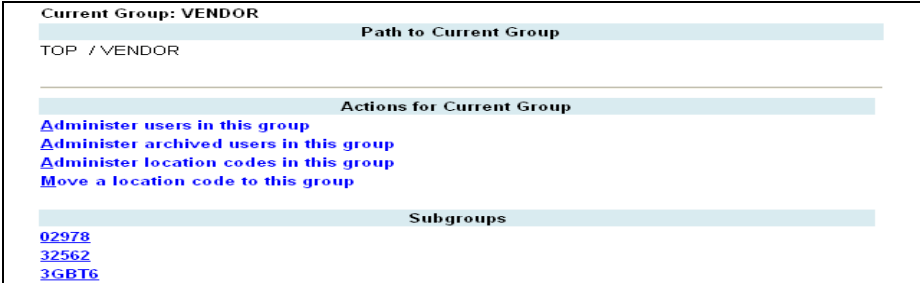*Continued on next page*

Administer users in this group, Continued

Procedure
(continued)

Step	Action
7	View user information. Current Group: VENDOR 	Userid	First Name	Last Name
MHnY55FD	Bianca	A'rmenta
E-mail Address	Commercial Telephone	DSN Telephone
wawf_undel@ecedi.nit.disa.mil	520-538-1919	
Title	Organization	Rank Grade
JITC	JITC	CIV
Certificate Issuer			 Return to List of Users Return to Group Structure
8	Click **Return to List of Users** to return to previous list **or** Click **Return to Group Structure** to return main page. *Tip: In this procedure we will Return to List of Users.*
9	Click **Role** under the "Actions". 	4	jackson2	333	333	Profile	Roles
5	MHnY55FD	Bianca	A'rmenta	Profile	Roles
6	4N727	Sheila	Adame	Profile	Roles	 *Tip: The list of user roles is displayed by Group Names, Cage codes or DoDAAC and extensions, active status, and comments and attachment*
10	Clicking on the **View** under Comments/Attachments will display any comments and attachments associated with the user. | Userid	First Name	Last Name	Role	Group	Location Code	Extension	Active Status	Comments	Attachments	Comments / Attachments
MHnY55FD	Bianca	A'rmenta	Group Administrator	VENDOR			Y	N	N	View	 Return to List of Users
11	Click **Return to List of Users**.

Administer archived users in this group

Introduction   Use the information from this link to view achieves users' information from their profile to their roles in that group.

Procedure   Follow the steps below to view achieve users information for the users in a group.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **Group Structure.** **[-] Group Administrator** **Group Structure** **Location Codes** **Group Lookup** **User Information** **Activation** **Activation Report** **Reset Password** **Reset Certificate** *Result: Current Group screen is displayed*.

Procedure (continued)

Step	Action
4	Click **Administer archived users in this group**. Current Group: VENDOR **Path to Current Group** TOP / VENDOR **Actions for Current Group** Administer users in this group Administer archived users in this group Administer location codes in this group Move a location code to this group **Subgroups** 02978 32562 3GBT6 *Result: This screen displays all achieve users available under this group. You can view the users Profile and/or Roles.*
5	On this screen you can the results are displayed ten a time, labels at the top of the screen indicate the current group and the total number of users, the current page number and page count are at the bottom of the page, a dropdown box and paging button allow you to select the next page to be viewed and you can sort the list of users by User ID by First Name, or by Last Name and in either ascending or descending alphabetical order. *Tip: To view user profile follow steps 6-8.* *To view user Role follow steps 9-11.*
6	Click **Profile** under "Actions" to view user's profile information. *Result: User Information screen is displayed with the user's registration information.*

Administer archived users in this group, Continued

Procedure
(continued)

Step	Action
7	View user information. **Current Group: VENDOR** 	Userid	First Name	Last Name
MHnY55FD	Bianca	A'rmenta
E-mail Address	Commercial Telephone	DSN Telephone
wawf_undel@ecedi.nit.disa.mil	520-538-1919	
Title	Organization	Rank Grade
JITC	JITC	CIV
Certificate Issuer			 Return to List of Users Return to Group Structure
8	Click **Return to List of Users** to return to previous list **or** Click **Return to Group Structure** to return main page. *Tip: In this procedure we will Return to List of Users and view Roles.*
9	Click **Role** under the "Actions". 	4	jackson2	333	333	Profile	Roles
5	MHnY55FD	Bianca	A'rmenta	Profile	Roles
6	4N727	Sheila	Adame	Profile	Roles	 *Tip: The list of user roles is displayed by Group Names, Cage codes or DoDAAC and extensions, active status, and comments and attachment*
10	Clicking on the View under Comments/Attachments will display any comments and attachments associated with the user. | Userid	First Name	Last Name	Role	Group	Location Code	Extension	Active Status	Comments	Attachments	Comments / Attachments
MHnY55FD	Bianca	A'rmenta	Group Administrator	VENDOR			Y	N	N	View	 Return to List of Users
11	Click **Return to List of Users**.

Administer location codes in this group

Introduction Use the information from this link to view the location code (DoDAAC/CAGE), email address and extensions in that group

Procedure Follow the steps below to view location code information for a group.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **Group Structure.** *Result: Current Group screen is displayed.*
4	Click **Administer location codes** in the group. *Result: The list of location codes is displayed*.

Administer location codes in this group, Continued
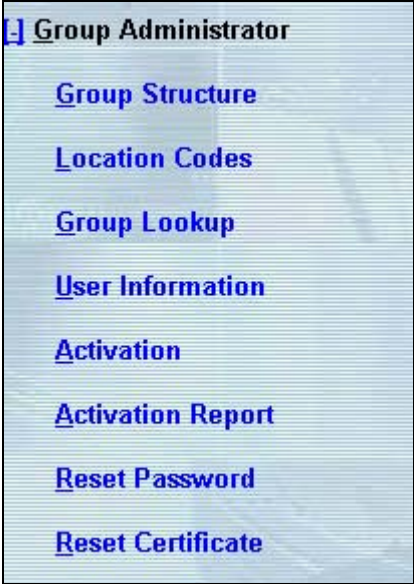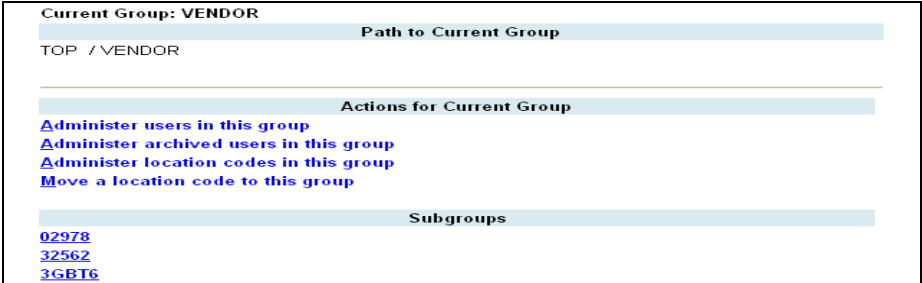
Procedure
(continued)

Step	Action
5	Click Email under "Action" to verify Primary and Secondary email settings. *Current Group: DFAS* *There is 1 location code in this group.* 	Location Code	Type	Org. Email	Action
1 HQ0101	DoDAAC	hq-wawf@dfas.mil	Email Extensions	 Return to Group Structure Page Help *Tip: On this screen you can the results are displayed ten a time, labels at the top of the screen indicate the current group and the total number of location codes. The current page number and page count are at the bottom of the page, a dropdown box and paging button allow you to select the next page to be viewed.*
6	Click **Return**. **Current Location Code: HQ0101** **Primary Organizational Email** **Email Settings** hq-wawf@dfas.mil All Emails **Secondary Organizational Email(s) Email Settings** Return Page Help
7	Click **Extension** to view the submenu **Current Group: VENDOR** **There are 660 location codes in this group.** 	Location Code	Type	Org. Email	Action
1	00144	CAGE Code	Joy.Dienst@adc.com	Extensions
2	001Z0	CAGE Code	wawfvend@dla.mil	Extensions
3	00779	CAGE Code	wawf_undel@ecedi.nit.disa.mil	Extensions
4	00929	CAGE Code	hq-wawf@dfas.mil	
5	00997	CAGE Code	wawf_undel@ecedi	
6	00D02	CAGE Code		
7	00SJ6			
8	00U			
9	012			
10	015			| |	Extension	Org. Email	EDA Access
1	EBEC	wawf_undel@ecedi.nit.disa.mil	N
2	EBEC2	wawf_undel@ecedi.nit.disa.mil	N	 Page 1 of 66 Go to: Page 2 >> Return to Group Structure

Move a location code to this group

Introduction   Use the information from this link to move a location code (DoDAAC/CAGE) from one group to another

Procedure   Follow the steps below to move a DoDAAC to another group

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **Group Structure.** ⊟ Group Administrator Group Structure Location Codes Group Lookup User Information Activation Activation Report Reset Password Reset Certificate *Result: Current Group screen is displayed.*
4	Click Move a location code to this group. Current Group: VENDOR Path to Current Group TOP / VENDOR Actions for Current Group Administer users in this group Administer archived users in this group Administer location codes in this group Move a location code to this group Subgroups 02978 32562 3GBT6 *Result: The list of location codes is displayed*.

Continued on next page

Move a location code to this group, Continued

Procedure
(continued)

Step	Action
5	Enter **DoDAAC/MAPAC** **Current Group: DFAS** DoDAA**C** / MAPAC HQ0101 Submit Cancel Page Help
6	Click **Submit.** *Result: You will receive a message.*
7	Click OK to move the group **or** Click Cancel to cancel the request **Current Group: ARMY HEAD QUARTERS** DoDAA**C** / MAPAC HAA031 Submit Cancel Page Help Microsoft Internet Explorer HAA031 is currently in the ARMY1 group. Do you wish to move HAA031 into the new subgroup? OK Cancel

Move a location code to this group, Continued

Procedure
(continued)

Step	Action
8	Click on Subgroups. Subgroups CENTER ACTIVITIES CONTRACTING FIELD ACTIVITIES *Tip: Once you have selected the group you wish to migrate, the Move this group option will appear.*
9	Click **Move this group.** Actions for Current Group Administer users in this group Administer archived users in this group Administer location codes in this group Move a location code to this group Move this group Subgroups
10	Select the new placement. Current Group: CENTER ACTIVITIES Please select the new placement in the group structure for the current group. Navigate to the group that the current group should be placed under by clicking on the group names. Path to Destination Group TOP / DFAS Subgroups COMMERCIAL PAY DFAS PURCHASES Submit Cancel Page Help *Tip: You will be prompted one final time by a pop-up box to finalize the migration.* *Result: The Path to the Destination Group will appear.*
11	Click **Submit**. *Tip: After completing the migration, the group migrated becomes a part of the new group structure. The activation status of users will not be affected after migrating the group structure.*
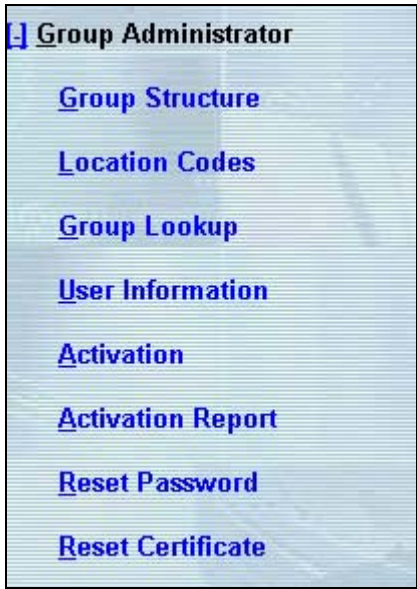
Location Codes

Introduction	This section you will learn how to perform the following tasks: ◊ Accessing the Location Codes administration screen ◊ Editing organizational e-mail addresses for location codes within the group ◊ Adding subgroup extensions to a location code within a group

Administer Location Codes

Introduction   Use the information from this link to access the various groups and locations codes within the group that are within the purview of their administrative functions.

Procedure   Follow the steps below to access the location codes administration screen.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **Location Codes.** **⊟ Group Administrator** **Group Structure** **Location Codes** **Group Lookup** **User Information** **Activation** **Activation Report** **Reset Password** **Reset Certificate** *Result: Current Group screen is displayed.*

Administer Location Codes, Continued

Procedure,
Continued

Step	Action
4	Select the groups from the drop down box that you wish to administer. **Select Group Path to Administer** DFAS / DFAS PURCHASES / FIELD ACTIVITIES / ACCOUNTING SERVICES Submit Page Help *Tip: The screen contains a drop down box that lists the groups that you may administer.* *Result: The Results screen will be displayed.*
5	Click **Submit.**
6	From this screen you will be able to administer location codes as described in the next two sections. **Current Group: DISA WAWF FIELD** There are 4 location codes in this group. |	Location Code	Type	Org. Email	Action	
1	HC1003	DoDAAC	wawf_undel@ecedi.nit.disa.mil	Email	Extensions
2	HC1004	DoDAAC	wawf_undel@ecedi.nit.disa.mil	Email	Extensions
3	HC1005	DoDAAC	wawf_undel@ecedi.nit.disa.mil	Email	Extensions
4	HC1013	DoDAAC	wawf_undel@ecedi.nit.disa.mil	Email	Extensions	 **Return to Select Group**

Edit Organizational Email

Introduction   Use the information from this link to assign and change e-mail addresses for location codes and their extensions.

Every location code has an organizational e-mail address. WAWF sends automatic e-mails to the organizational e-mail addresses when WAWF documents are submitted, inspected, accepted, certified, processed, resubmitted, or rejected.

Procedure   Follow the steps below to assign or change the organizational e-mail address associated with a location.

Step	Action
1	Follow steps 1 -6 from section "Access the Location Codes Administration Screen" section.
2	Click the **Email** next to the location you wish to edit. **Current Group: DISA WAWF FIELD** There are 4 location codes in this group. 	Location Code	Type	Org. Email	Action	 1 HC1003 DoDAAC wawf_undel@ecedi.nit.disa.mil **Email Extensions** 2 HC1004 DoDAAC wawf_undel@ecedi.nit.disa.mil **Email Extensions** 3 HC1005 DoDAAC wawf_undel@ecedi.nit.disa.mil **Email Extensions** 4 HC1013 DoDAAC wawf_undel@ecedi.nit.disa.mil **Email Extensions** **Return to Select Group** *Result: The organization e-mail screen will open.*

Edit Organizational Email, Continued

Procedure,
Continued

Step	Action
3	To change or edit the e-mail address, place your cursor in the text box and make the necessary changes. **Current Location Code: HQ0306** **Primary Organizational Email** — DCH-CRFO-WAWF@dfas.mil — **Email Options**: ○ No Emails ○ Negative Emails ⊙ All Emails **Secondary Organizational Email(s)** — **Email Options**: ○ No Emails ○ Negative Emails ⊙ All Emails ○ No Emails ○ Negative Emails ⊙ All Emails ○ No Emails ○ Negative Emails ⊙ All Emails [Submit] [Cancel] [Page Help] *Tip: The e-mail screen contains the current e-mail assigned to the location. The title at the top of the screen indicates the location code of the e-mail address that is being modified.* *You can change the primary organizational email or add and change any secondary organizational e-mail(s). You can also change e-mail option.*
4	Click **Submit.** *Result: The current group screen will be displayed. The change is successful. The updated organizational e-mail address is reflected in the location code information.*
5	Click **Return to Select Group** to select another group **Current Group: DISA WAWF FIELD** There are 4 location codes in this group. 	Location Code	Type	Org. Email	Action	 1 HC1003 DoDAAC chris.jones@wpafb.af.mil Email Extensions 2 HC1004 DoDAAC wawf_undel@ecedi.nit.disa.mil Email Extensions 3 HC1005 DoDAAC wawf_undel@ecedi.nit.disa.mil Email Extensions 4 HC1013 DoDAAC wawf_undel@ecedi.nit.disa.mil Email Extensions **Return to Select Group**

Add Subgroup Extensions

Introduction   Use the information from this link to subdivide the location codes into extensions to help organize the users within a location code.

While some users should have access to entire DoDAAC or CAGE Code contents, others should have access only to the data they need. You can create extensions that subdivide the DoDAAC or CAGE Code into smaller units according to your Agency's business rules.

If an extension is created, it is appended to the name of the DoDAAC or CAGE Code.

When users having an extension register, they need to re-register for the new DoDAAC + extension or new CAGE Code + extension.

When a document is created or submitted by or to an organization assigned an extension, its location code is referred to as DoDAAC + extension or CAGE Code + extension. Every extension can be assigned an e-mail address when it is created or updated with a new email address after activation. Automatic e-mail notifications will be delivered only to the address specifically associated with the extension.

Caution: GAMs electing to add an extension to an existing Group must take into account that if an extension is added, the Vendors submitting documents to that Group must be notified to use the associated Location Code and extension either via a contract modification, or via an agreement. Creation of an arbitrary extension may result in mis-routed documents or the inability of the Vendor to submit a document if there are no active users at the Location Code level.

Add Subgroup Extensions

Procedure   Follow the steps below to add an extension to the location code

Step	Action
1	Follow steps 1 -6 from section "Access the Location Codes Administration Screen" section.
2	Select the group to which you wish to add extensions. *Result: The Current Group screen appears. The list of location codes within this group is displayed. The table provides a link to view or modify an existing extension or add a new extension to the selected location code.*
3	Click **Extensions**. *Tip: Each extension can have its own organizational e-mail.* *Results: The extensions screen is displayed.*

Continued on next page

Add Subgroup Extensions, Continued

Procedure
(continued)

Step	Action
4	Click **Create Extensions** to add/change an extension. Current Location Code: HQ0104 There are 2 extensions for this code. |	Extension	Org. Email	Actions
1	34339	vanessa.davis@dfas.mil	Update
2	HQ0104	chuck.ruoff@dfas.mil	Update	 [Create Extension] [Return] [Page Help] *Results: The Add Extensions Screen is displayed*.
5	Type the new extension name and organization e-mail address. Current Location Code: HQ0104 Extension	Primary Organizational Email	Email Options ○ No Emails ○ Negative Emails ⊙ All Emails Secondary Organizational Email	Email Options ○ No Emails ○ Negative Emails ⊙ All Emails ○ No Emails ○ Negative Emails ⊙ All Emails ○ No Emails ○ Negative Emails ⊙ All Emails [Submit] [Cancel] [Page Help] *Tip: The current location code is displayed at the top of the page*.
6	Click **Submit**. *Results: The Extensions screen reopens. The new extension is added to the list of extensions for the location code.*

Add Subgroup Extensions, Continued

Procedure
(continued)

Step	Action
7	From here, you can add more extensions by clicking on the "Create New Extensions" link, or you may return to the location codes list to continue performing administrative actions by clicking on the "Return to Location Codes" link at the bottom of the page

Current Location Code: HC1001

There are 2 extensions for this code.

	Extension	Org. Email	Actions
1	1111	wawf_undel@ecedi.nit.disa.mil	Email
2	2111	jamesj@ctcgsc.org	Email

Create New Extension
Return to Location Codes

Group Lookup
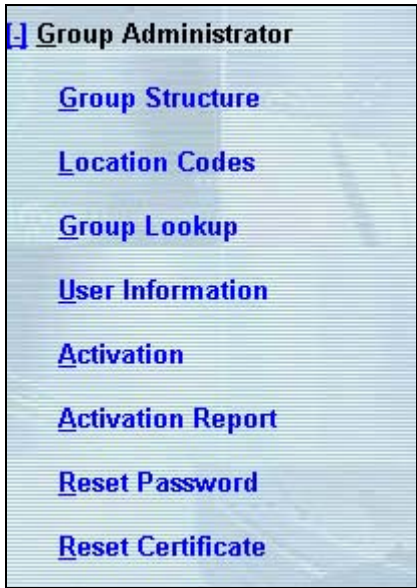
Introduction   In this section you will learn how to perform the following task:

◊   View information on the GAM(s) associated with a location code

Access the Group Lookup Information

Procedure   Follow the steps below to access the group lookup submenu and display Group Name and GAM(s) associated with the location.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **Group Lookup.** **[-] Group Administrator** **Group Structure** **Location Codes** **Group Lookup** **User Information** **Activation** **Activation Report** **Reset Password** **Reset Certificate** *Result: The Group Lookup By Location Code screen opens.*

Continued on next page

Procedure,
Continued

Step	Action
4	Enter in the location Code (**DoDAAC or CAGE Code**) for which you want the Group Name and GAM information.
5	Click **Continue**. *Results: The Group Lookup By Location Code screen opens.*
6	View the list of Group Administrators, as is the associated group e-mail and phone number(s) for each GAM.
7	Click **Return**.

User Information

Introduction   The User Information option provides a means for locating a specific user via a search. Once located, the GAM may view detailed information in the user's profile (including telephone numbers and e-mail address) and his/her functional roles within the application.

Available information is limited to users within the GAM's sphere of responsibility (i.e. Groups the GAMs have been authorized to administer).

In this section you will learn how to perform the following tasks:

◊   Access the User Information screens

◊   Use the Search Screen to submit specific search criteria and manipulate search results

◊   Use the Results Screen to:

◊   View user profile information

◊   View a list of roles for which the user is registered

Guidelines for Initiating a Search   Here are some guidelines for using the Search Screen:

◊   You must enter data in at least one search field

◊   The data in multiple search fields will be combined, and only records that match all entered criteria will be returned

◊   If there are more than 500 records found that match the entered criteria; you will be asked to enter additional information to narrow the search.

Search Methods   There are three methods for searching database records.

      ◊ Search using drop down boxes to select specific criteria in the
          following fields:

      ◊ Group Name

      ◊ Role

      ◊ Active Status

      ◊ Search using partial values in the following fields:

      ◊ User ID

      ◊ First Name

      ◊ Last Name

      ◊ Location Code

      ◊ Extension

      ◊ Search using a combination of selected and partial values in single
          or multiple fields.

Procedure Using Specified Criteria

To do advanced searches to more narrowly define the population returned, you may use selection criteria in the following fields:

◊ User ID

◊ First Name

◊ Last Name

◊ Location Code

◊ Extension

You may use specific values in the fields or you may use partial values to extract relevant data. In the drop down boxes next to the fields listed above, you can specify how to search on the partial value entered.

◊ **Is exactly** – used when you know the specific value contained in the given field.

◊ **Begins with** – used when you know what the field begins with, but not what is contained in the rest of the field. (Example: the field begins with a known DoDAAC, but also contains a name not known to you.)

◊ **Contains** – used when you know a particular value is contained within the field, but not where.

◊ **Ends with** – used when you know a field ends with a specific value, but you are not sure what is contained in the rest of the field.
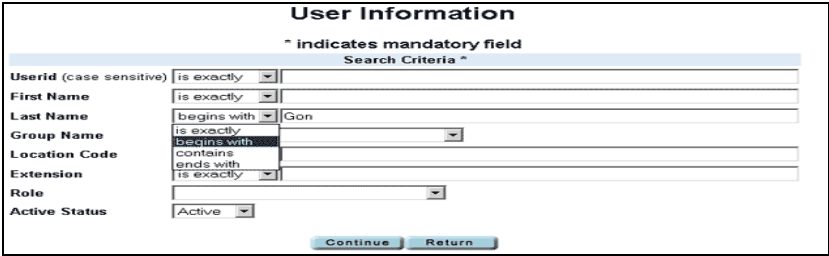
Use the procedure below to query using specified criteria to display a list all users sharing the selected criteria.

Access User Information Screen

Introduction   Use the information from this link to access the user information

Procedure   Follow the steps below to access the user information screens.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **User Information.** *(Group Administrator menu showing: Group Structure, Location Codes, Group Lookup, User Information, Activation, Activation Report, Reset Password, Reset Certificate)* *Results: The User Information screen opens.*
4	Choose the field you wish to query on. Enter either the full value of the field or enter a partial value and select a companion statement in the drop down box. *(User Information search criteria screen)* **Results: A list of users matching the specified criteria is displayed** *Tip: You may use any combination of criteria to extract a list of values*.

Manipulate Search Results

Introduction   You can sort the records in the list of users by User ID, by First Name, or by Last Name in either ascending or descending alphabetical order.

Search Results - Display Limitations   When your search criteria have been submitted, the Results Screen displays a list of user records that fits your search criteria.

◊   The results are displayed ten at a time.

◊   A label at the top of the screen indicates the total number of records.

◊   At the bottom of the page is the current page number and page count.

◊   A drop down box and paging button allow you to select the next page to be viewed.

Procedure   Follow the steps below to manipulate search results.

Step	Action
1	Follow steps 1 – 4 in section "Access User Information Screen"
2	Click on the first Sort by drop down box. Select the field you wish to sort by (User ID, First Name, or Last Name). 6 users found. **User Information** Sort by: Userid ascending **Sort** Userid First Name Last Name **First Name** **Last Name** **Actions** 1 chisSykes Chris Sykes **Profile** **Roles** 2 jmulligan Jerry Mulligan **Profile** **Roles** 3 LesterTony Tony Lester **Profile** **Roles** 4 pat.gonsalves Pat Gonsalves **Profile** **Roles** 5 pat.gonsalves_msp Pat Gonsalves **Profile** **Roles** 6 vendGam3 Jenny James **Profile** **Roles** **Return to Search Screen**
3	Click on the second Sort by drop down box. Select the order in which you wish to display data (ascending or descending).
4	Click the sort button. Result: The data will be resorted according to the criteria specified

View User Profile Information

Introduction   The Group Administrator has the ability to view the registration information of each user. However, he or she cannot change or edit the information.

The User Information Screen displays the user's registration information:

◊   User ID and name

◊   Addresses and telephone numbers

◊   Rank

◊   Title and job description

◊   Certificate number

Procedure   Follow the steps below to view user profile information.

Step	Action
1	Follow directions in the previous sections to produce a list of users.
2	Click **Profile**. Results: The User Information screen containing the selected user's data is displayed.

View User Profile Information, Continued

Procedure
(continued)

Step	Action
3	View the user's data, you may either return to the previous list of users, return to the search screen to conduct a new search by selecting the appropriate link or edit the users Profile at the bottom of the screen.
4	Click **Edit Profile**.
5	Click Submit after making changes to a user's profile.

View User Role Information

Introduction   The Group Administrator has the ability to view the roles assigned to each user. However, he or she cannot change or edit the information on this screen.

The Roles Screen displays all roles the user is registered for (including roles in other groups). Additionally, the following information is displayed:

◊   Group Names

◊   CAGE Codes or DoDAACs and extensions

◊   Active Status

Tip: Group Administrators do not have a CAGE code or DoDAAC assigned to their role. As a GAM, they have administrative abilities for groups that are made up of multiple CAGE codes or DoDAACs.

Procedure   Follow the steps below to view user role information.

Step	Action
1	Follow directions in the previous sections to produce a list of users.
2	Click **Roles**. **User Information** 11 users found. Sort by: Userid / ascending / Sort Userid First Name Last Name Actions 11 vendGam3 Jenny James Profile Roles Page 2 of 2 Go to: Page 1 >> Return to Search Screen *Results: The User Information screen containing the selected user's data is displayed.*

View User Role Information, Continued

Procedure
(continued)

Step	Action
3	Click on the Sort by drop down box to sort the records,. This drop down box sorts the records in ascending alphabetical order by any of the fields available on the screen. *Tip: You can sort by User ID, First name, Last Name, Role, Group, Location Code, Extension, and Active Status.*
4	Click Return to List of Users after reviewing the User's role data.

Activation

Introduction   The User Activation option provides the primary means for the GAM to approve a user's access to the application for Location Codes for which he/she is responsible. After searching for a user via the standard search windows, the results are presented to the GAM matching the search criteria.

From this menu, the GAM can maintain access to the Location code (DoDAAC) and may change any user's status from active to inactive or vice versa by clicking the check box next to the user's information. Comments are not required. More than one user's statuses can be changed by clicking in the check box on all user accounts that require a change of status.

Caution: If a GAM grants access to a person from a third party (contract worker) doing work for the GAM's Activity (such as someone hired by contract to perform receipt and inspection at a supply center), that individual has access by role to ALL documents under the users DoDAAC. This access will provide the contractor with full access to invoices, receiving reports, contracts and linked payment information under the individual contract number submitted to WAWF.

In this section you will learn how to perform the following tasks
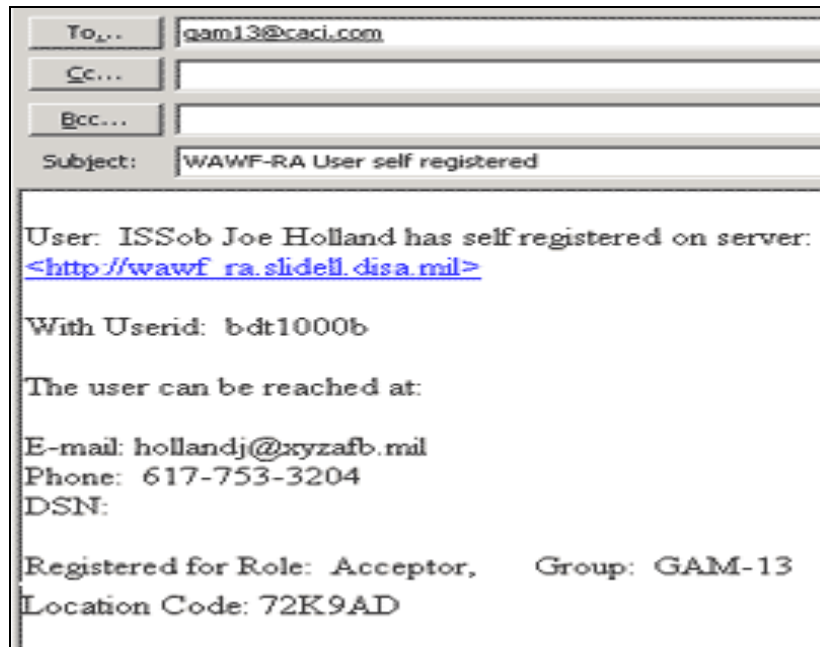
◊   Activating User Accounts

◊   Deactivating User Accounts

Reactivating User Accounts

Activating User Accounts

Introduction   The Activation process begins when you receive an automatic e-mail notification from WAWF that a new user has self-registered for the group. See sample e-mail below.

```
To...     gam13@caci.com
Cc...
Bcc...
Subject:  WAWF-RA User self registered

User: ISSob Joe Holland has self registered on server:
<http://wawf_ra.slidell.disa.mil>

With Userid: bdt1000b

The user can be reached at:

E-mail: hollandj@xyzafb.mil
Phone: 617-753-3204
DSN:

Registered for Role: Acceptor,     Group: GAM-13
Location Code: 72K9AD
```

Gaining access to WAWF is a two step process. First a user registers using the self-registering process, then the GAM will validate and activate the users' account
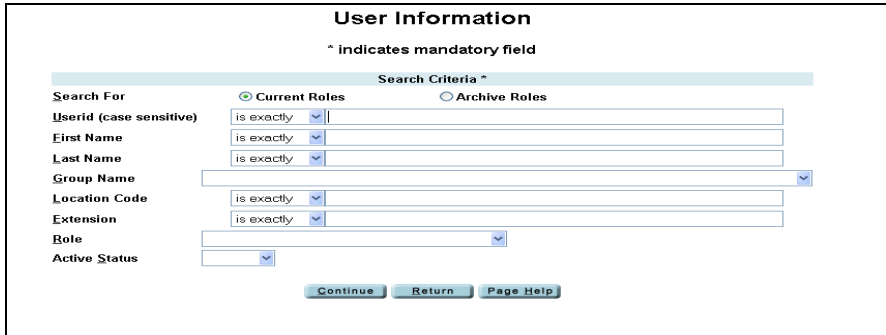
Procedure   Follow the steps below to activate user accounts.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.

Activating User Accounts, Continued

Procedure
(continued)

Step	Action
3	Click on **Activation.** *Result: The User Information opens.*
4	Enter the User ID or any other criteria that will search for the user's record found in the e-mail. *Tip: It is required that search criteria be entered into at least one search field.*
5	Click **Continue**. *Result: The user's registration information is displayed.*

Activating User Accounts, Continued

Procedure
(continued)

Step	Action
6	Verify the DD Form 2875 information against the user's registration information is attached. ***Tip: If the User Activation data in WAWF matches the DD Form 2875, you may continue with the activation process. The new government user must provide you with a DD Form 2875.*** ***Result: The user's registration information is displayed Activation screen that opens shows the user's registration information***

Activating User Accounts, Continued

Procedure
(continued)

Step	Action
7	Click in the **Change Status** checkbox to activate the user. The Active Status is N, which means (No) the user is not active in WAWF. *Tip: The Comment field is optional, however, if filled in, it can provide useful information. The GAM may type in a comment describing how the user was authorized and how the registration information was authenticated. In the example above, the Government GAM referenced the approved DISA Form 41 9 this form was the predecessor to the DD Form 2875). Vendor GAMs can reference their own internal approval process. Comments are not visible or maintained in WAWF after submission.*
8	Click **Submit**.

Activating User Accounts, Continued

Procedure
(continued)

Step	Action
9	You are informed that the activation was successful. **User Activation** **Activation/Deactivation was successful!** | Userid	First Name	Last Name	Role	Group	Location Code	Extension	New Status | | bdt1000b | Joe | Holland | Acceptor | GAM-13 | 72K9AD | | Active | *Results:* ◊ *The New Status field says "Active".* ◊ *The WAWF system automatically sends an e-mail to the activated user with a one-time password for all initial activations.* ◊ *The user will be added to the Active Status list generated by the User Information search page.* *Tip: Temporary password will not be generated for addition of additional roles or DoDAACs.*
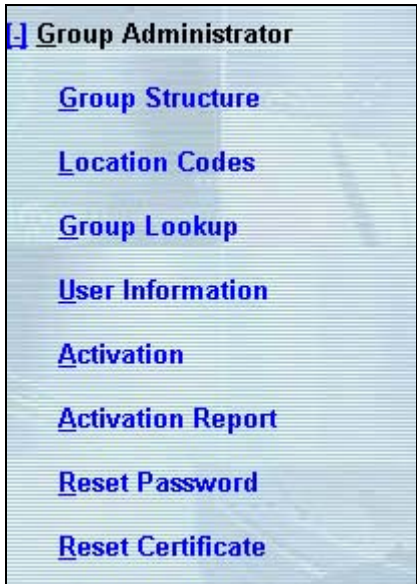
Deactivating User Accounts

Introduction   Deactivation of user accounts will be performed in accordance with the Activity's business rules. GAMS's are responsible for reviewing the users account on an on going basis. However, it is recommended that when a member leaves their assigned activity that the GAM should prevent unauthorized access by deactivating the users account.

Procedure   Follow the steps below to deactivate user accounts.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **Activation.**

Continued on next page

Deactivating User Accounts, Continued

Procedure
(continued)

Step	Action
4	Enter the User ID or any other criteria that will search for the user's record found in the e-mail. *Tip: It is required that search criteria be entered into at least one search field.*
5	Click **Continue**. *Result: The user's registration information is displayed.*
6	Click in the **Change Status** checkbox to deactivate the user The Notice that the **Active Status** field has a "**Y**" in it, which means (Yes) the user is active in WAWF.

Procedure
(continued)

Step	Action
7	Click **Submit**. ![User Activation form] *Tip: Although the Comment is an optional field, it is useful for documenting the method of verification or the reason the user is being deactivated; for example, transfer or promotion.*
8	You are informed that the deactivation was successful. ![User Activation successful] *Results:* ◊ *The New Status field is changed to "Inactive".* ◊ *The user is added to the Inactive Status list generated by the User Information search page.*

Reset User Password

Introduction　　GAMs are called upon to reset passwords in cases where the user cannot. The rules for resetting a password are as follows:

◊　A group administrator can reset user's password for all users assigned under their group(s)

◊　A group administrator may not reset a password for a user who is registered with a certificate.

The group administrator will never see the new password. The new, single-use temporary password will be sent via e-mail to the user's e-mail account of record in WAWF.

In this section you will learn how to perform the following tasks:

◊　Resetting User Passwords

Procedure　　Follow the steps below to reset user passwords.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **Reset Password.**

<table>
<tr><td>

[-] Group Administrator

Group Structure

Location Codes

Group Lookup

User Information

Activation

Activation Report

Reset Password

Reset Certificate

</td></tr>
</table>

Deactivating User Accounts, Continued

Procedure
(continued)

Step	Action
4	Enter the User ID of the user whose password needs to be reset. **Reset Password** * indicates mandatory field Userid * lesterTony Continue *Result: The Profile Information screen opens.*
5	Click **Continue**.
6	Verify the information on this screen to ensure the user's identity before resetting the password. Once verified, **Reset Password** Profile Information <table><tr><th>First Name</th><th>Last Name</th><th>Commercial Phone</th><th>DSN Phone</th><th>Email</th><th>Rank</th><th>Title</th><th>Job Description</th></tr><tr><td>Anthony</td><td>Lester</td><td>999-999-9999</td><td></td><td>tony.lester@milsupply.com</td><td>CIV</td><td>Billing Specialist</td><td>Invoice customers</td></tr></table> Reset Password

Deactivating User Accounts, Continued

Procedure
(continued)

Step	Action
7	Click **Reset Password**. *Results:* ◊ *Password change is submitted.* ◊ *Success screen is displayed*
8	The user receives a system-generated e-mail containing a new one-time password. *Tip: After logging on to WAWF with the one-time password, the user is required to provide a new password.*

Reset User Certificate
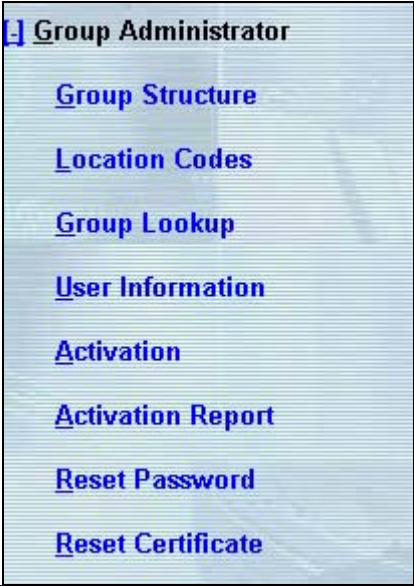
Introduction   This section contains procedures for resetting user certificates. There are several reasons a certificate user would request to have their certificate reset.

    ◊   Their current certificate has expired or is no longer valid

    ◊   They have received a new certificate

    ◊   They have successfully logged on with their certificate previously, but are now having difficulty logging on with their certificate

The reset certificate process begins when you receive notification that a WAWF user requires a certificate reset.
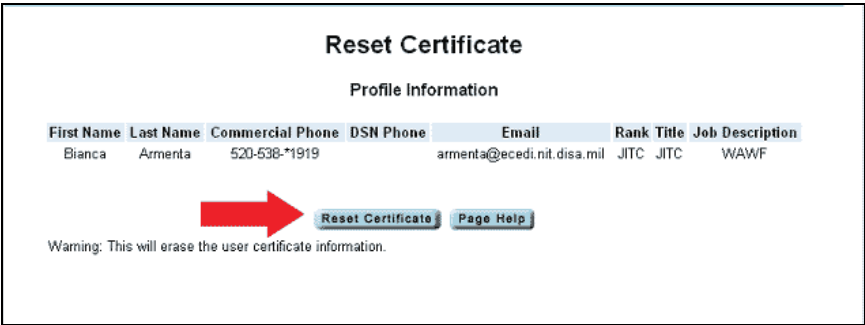
Procedure   Follow the steps below to reset a user's certificate.

Step	Action
1	**Logon** to WAWF
2	Click the (+) next to **Group Administrator** to expand.
3	Click on **Reset Certificate.** **⊟ Group Administrator** **Group Structure** **Location Codes** **Group Lookup** **User Information** **Activation** **Activation Report** **Reset Password** **Reset Certificate**

Reset User Certificate, Continued

Procedure
(continued)

Step	Action
4	Type in the User ID of the user whose certificate needs to be reset. **Reset Certificate** * indicates mandatory field Userid * VGgXTLIS Continue Page Help
5	Click **Continue**. Result: The Reset Certificate screen is displayed
6	Verify the data on this screen to ensure users identity before resetting the certificate. **Reset Certificate** Profile Information First Name Last Name Commercial Phone DSN Phone Email Rank Title Job Description Bianca Armenta 520-538-*1919 armenta@ecedi.nit.disa.mil JITC JITC WAWF Reset Certificate Page Help Warning: This will erase the user certificate information.
7	Click **Reset Certificate**. Results: The reset certificate success screen is displayed

Procedure
(continued)

Step	Action

8	The Reset Certificate button initiates three WAWF system actions:
	
	◊ A new one-time use password is generated and sent via e-mail to the user (see sample e-mail below)
	
	◊ The user's certificate information is erased from the WAWF system
	
	◊ The user's logon method is changed to "User ID and Password."
	
	From: wawf_undel@ecedi.nit.disa.mil
	To: armenta@ecedi.nit.disa.mil
	Cc:
	Subject: WAWF-RA Certificate Reset Notification
	
	`Your certificate has been reset by a WAWF-RA administrator.`
	
	`Your one-time password for logging on to WAWF is 2#Va4GV72`

9	The user may then initiate a profile update to revert back to use of a certificate.

Appendix A – Sample DD Form 2875

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

PRINCIPAL PURPOSE: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES: None.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST		DATE
☐ INITIAL ☐ MODIFICATION ☐ DELETION ☐ USER ID _____		

SYSTEM NAME *(Platform or Applications)*	LOCATION *(Physical Location of System)*

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*	2. SOCIAL SECURITY NUMBER

3. ORGANIZATION	4. OFFICE SYMBOL/DEPARTMENT	5. PHONE *(DSN or Commercial)*

6. OFFICIAL E-MAIL ADDRESS	7. JOB TITLE AND GRADE/RANK

8. OFFICIAL MAILING ADDRESS	9. CITIZENSHIP	10. DESIGNATION OF PERSON

USER AGREEMENT *(Complete Block 29 or 30 as appropriate)*

I accept the responsibility for the information and DoD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DISA/DoD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*

☐ I have completed Annual Information Awareness Training.   DATE _____

11. USER SIGNATURE	12. DATE

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS

14. TYPE OF ACCESS REQUIRED:
☐ AUTHORIZED   ☐ PRIVILEGED   LEVEL OF CERTIFICATION CLEARANCE _____

15. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED   ☐ CLASSIFIED *(Specify category)*
☐ OTHER _____

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. ☐	16a. EXPIRATION DATE FOR ACCESS *(Specify date if less than 1 year)*

17. SUPERVISOR'S NAME *(Print Name)*	18. SUPERVISOR'S SIGNATURE	19. DATE

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER

21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE

22. SIGNATURE OF IAO	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE

26. SYSTEM ADMINISTRATOR:
I have completed my Annual Requirement for Information Assurance awareness.

☐ YES   ☐ NO   DATE _____

DD FORM 2875, MAR 2004   REPLACES DISA FORM 41, WHICH IS OBSOLETE.   ☐ Reset

Appendix A – Sample DD Form 2875, Continued

27. OPTIONAL INFORMATION

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION		28a. CLEARANCE LEVEL	
28b. IT LEVEL DESIGNATION	28c. DATE	28d. TYPE OF DESIGNATION	
29. VERIFIED BY *(Print name)*		30. SIGNATURE	31. DATE

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED	PROCESSED BY *(Print name and sign)*	DATE
DATE REVALIDATED	REVALIDATED BY *(Print name and sign)*	DATE

DD FORM 2875 (BACK), MAR 2004

Reset

Appendix A – Sample DD Form 2875, Continued

INSTRUCTIONS

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

(1) Name. The last name, first name, and middle initial of the user.

(2) Social Security Number. The social security number of user.

(3) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).

(4) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).

(5) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.

(6)Official E-mail Address. The user's official e-mail address.

(7) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.

(8) Official Mailing Address. The user's official mailing address.

(9) Citizenship. The user's citizenship status.

(10) Designation of Person.

IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.

(11) User's Signature. User must sign the DD Form X455 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the GovernmentSsponsor.

(13). Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)

(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.

(16) Verification of Need to Know. To verify that the user requires access as requested.

(16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.

(17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.

(18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.

(19) Date. Date supervisor signs the form.

(20) Supervisor's Organization/Department. Supervisor's organization and department.

(20a) E-mail Address. Supervisor's e-mail address.

(20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form X455.

(22) Signature of IAO. Signature of the IAO or sponsoring office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form X455.

(26) System Administrator. Place an "X" in the appropriate box and indicate date Information Assurance requirement was completed.

(27) Optional Information. This item is intended to add site specific information, as required.

C. PART III: Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Clearance Level. The user's current security clearance level (Secret, Top Secret).

(28b) IT Level Designation. The user's ADP designation (ADP1, ADP3, etc.).

(28c) Date. Date of last investigation.

(28d) Type of Designation. The user's last ADP designation (ADP1, ADP2, etc.).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Signature. The Security Manager or representative signature indicates that the above clearance and investigation information has been verified.

(31) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.

DD FORM 2875 INSTRUCTIONS, MAR 2004

Cd

Appendix B – Sample GAM Appointment Letter

[Enter the Group Administrator Manager's name]
[Enter the Group Administrator Manager's email address]
[Enter the Group Administrator Manager's phone number]

1.   You are hereby appointed a (select "primary" OR "alternate") Group Administrator for the WAWF-RA application. Your span of control includes the following DODAAC (or CAGE) codes. [List of DODAAC(s) or CAGE codes must be listed here or attached]

2.   You are responsible for the following activities:

   a. Establish hierarchical sub-groups for managing user accounts, as necessary.

   b. Establish organizational e-mail for each DODAAC (or CAGE) code and submit these to the WAWF-RA Customer Service Center

   c. Instruct registrants within your span of control to register.

   d. Activate and update users in your group within one business day of request.

   e. Ensure that requests for user access are valid and assign access at the appropriate authorization and privilege level.

   f. Ensure that subordinate group administrators and alternates are created, as necessary.

3. As a group administrator, you are a critical part of maintaining system security because you have the ability to grant access to users. You are responsible for validating the "need to know" of the users that you activate, and would be responsible for de-activating an invalid user. Ensure that users are who they say they are and that only the privileges necessary to accomplish their job duties are associated with this activated user account.

4. If a user's account needs to be de-activated, you are responsible for de-activating that account by following the procedure in the Group Administrator Manual (GAM). The Manual can be downloaded from WAWF-RA production or from training site. See link to Software Users Manual.

Signature Block:

Service/Agency Official (or Vendor EB POC)
Email Address
Phone Number